

1/22

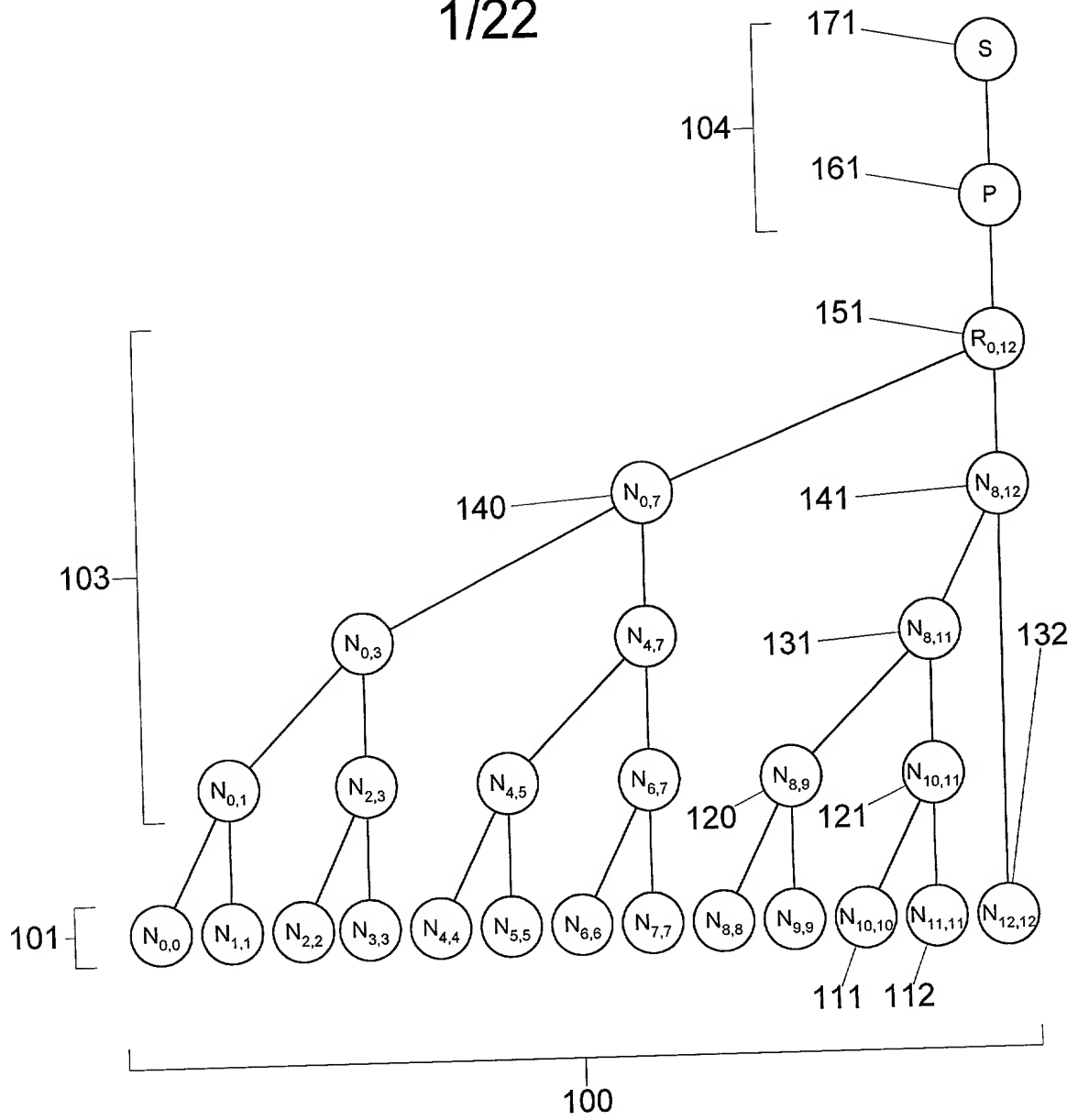


Figure 1

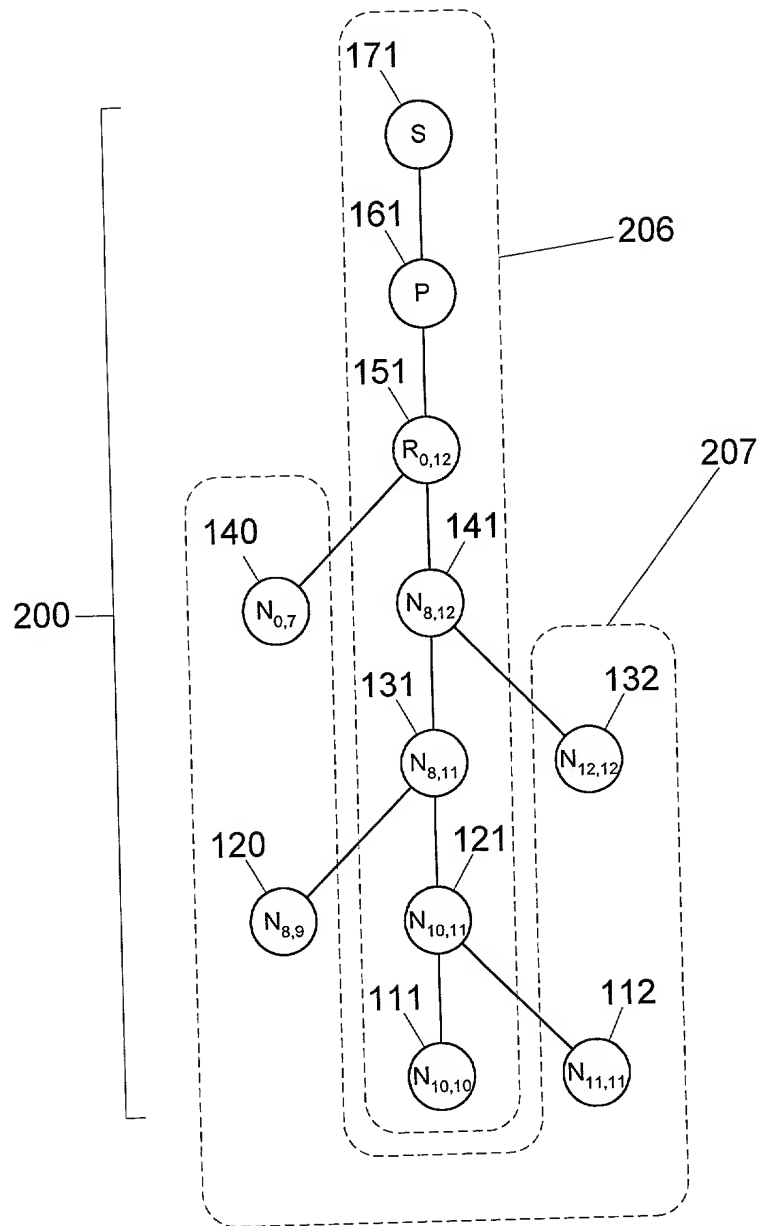


Figure 2

3/22

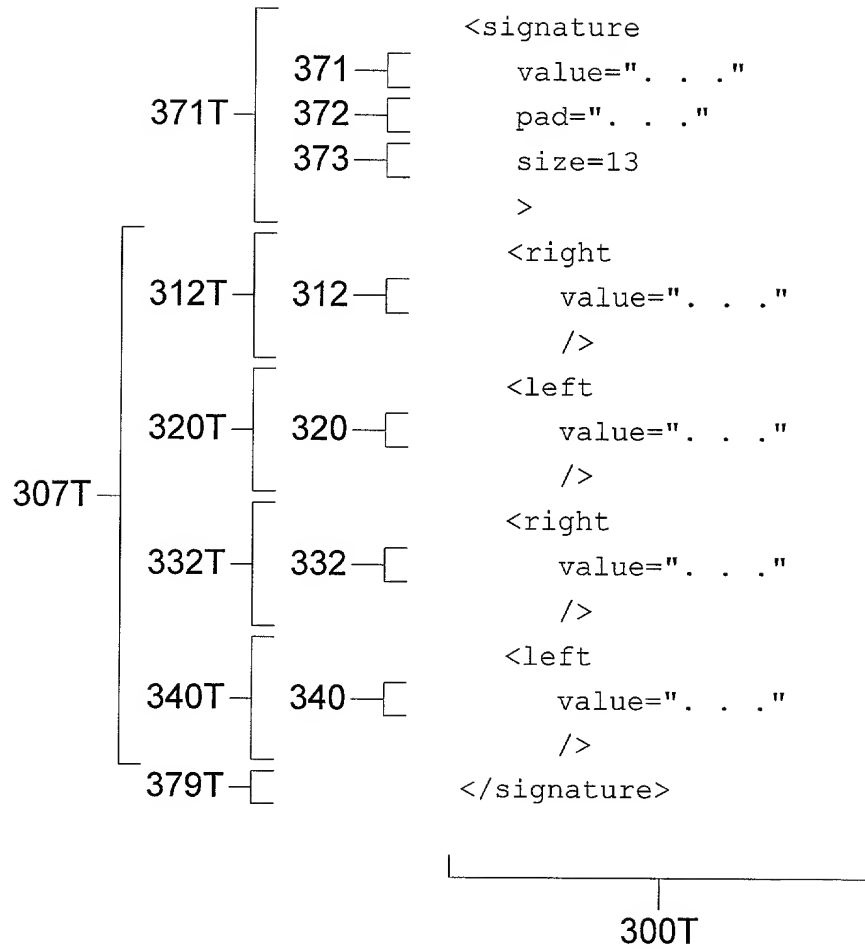


Figure 3

4/22

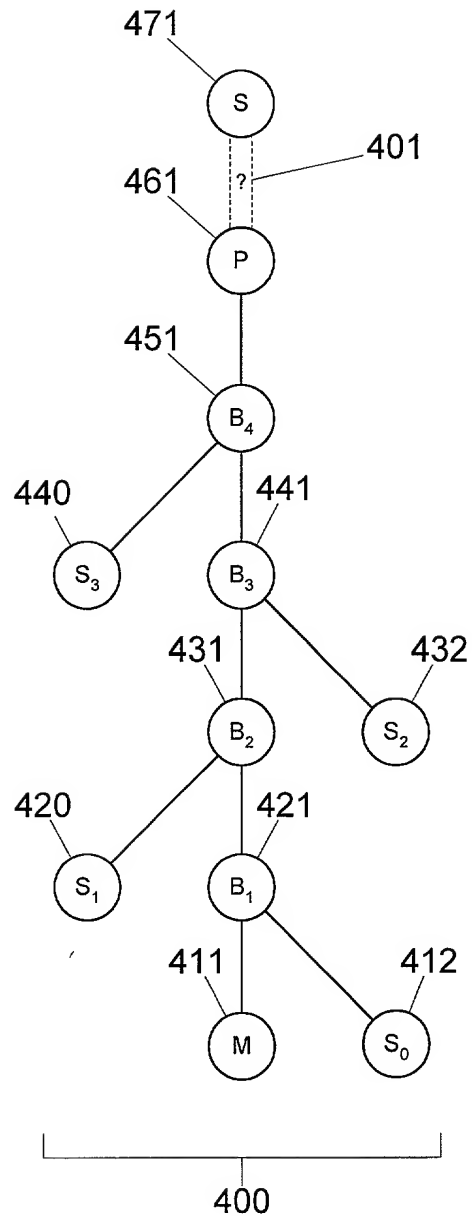


Figure 4

5/22

- 5.1 \mathbf{N} : the natural numbers 0, 1, 2, 3, ...
- 5.2 L : a security parameter for cryptographic hash functions
- 5.3 $\mathbf{H} = \Sigma^L$ = set of all bit strings of length L
- 5.4 Σ^* = set of all bit strings of any length
- 5.5 $F : \Sigma^* \rightarrow \mathbf{H}$: a cryptographic hash function of output length L
- 5.6 P : a security parameter for a public key signature scheme
- 5.7 $\mathbf{J} = \Sigma^P$ = set of all bit strings of length P
- 5.8 \mathbf{K}_E : the space of private keys of the signature scheme
- 5.9 \mathbf{K}_D : the space of public keys of the signature scheme
- 5.10 $S_{EG} : \mathbf{K}_E \times \mathbf{J} \rightarrow \mathbf{J}$: the signing operation of a private key
- 5.11 $V_{EG} : \mathbf{K}_D \times \mathbf{J} \times \mathbf{J} \rightarrow \mathbf{B}$: the verification predicate of a public key
- 5.12 \mathbf{H}^+ : positive length sequences of values in \mathbf{H}
- 5.13 $\# : \mathbf{H}^+ \rightarrow \mathbf{N}$: the length of a sequence
- 5.14 $\overline{M} = \{M_i\} \in \mathbf{H}^+$: a sequence of messages
- 5.15 $n = \# \overline{M}$: the number of input messages; also the size of a hash tree
- 5.16 $\text{Base10} : \mathbf{N} \rightarrow \Sigma^*$: represents a number as an ASCII base-10 integer
- 5.17 $\text{Base64} : \mathbf{N} \rightarrow \Sigma^*$: represents a number as an ASCII base-64 integer
- 5.18 quote : a constant, the ASCII quote character
- 5.19 $+: \Sigma^* \rightarrow \Sigma^*$: string concatenation
- 5.20 $\mathbf{B} = \{true, false\}$: boolean values

Figure 5

6/22

- 6.1 $\mathbf{T}_n \subset \mathbf{N} \times \mathbf{N}$: the set of positions in an ordered tree of size n
- 6.2 $K : \mathbf{N} \times \mathbf{N} \rightarrow \mathbf{N} : \langle i, j \rangle \mapsto \min \{ k \mid j - i < 2^k \}$
- 6.3 $\mathbf{T}_n = \{ \langle i, j \rangle \mid 0 \leq i \leq j \leq n-1 \wedge (2^{K(\langle i, j \rangle)} \mid i) \wedge j = \min(i + 2^{K(\langle i, j \rangle)} - 1, n-1) \}$
- 6.4 $\mathbf{T}_n^+ = \{ \langle i, j \rangle \mid \langle i, j \rangle \in \mathbf{T}_n \wedge i \neq j \}$: the parent nodes in the tree
- 6.5 $\mathbf{T}_n^- = \{ \langle i, j \rangle \mid \langle i, j \rangle \in \mathbf{T}_n \wedge \langle i, j \rangle \neq \langle 0, n-1 \rangle \}$: the child nodes in the tree
- 6.6 $\text{Left}_n : \mathbf{T}_n^+ \rightarrow \mathbf{T}_n^- : \langle i, j \rangle \mapsto \langle i, i + 2^{K(\langle i, j \rangle)-1} - 1 \rangle$
- 6.7 $\text{Right}_n : \mathbf{T}_n^+ \rightarrow \mathbf{T}_n^- : \langle i, j \rangle \mapsto \langle i + 2^{K(\langle i, j \rangle)-1}, j \rangle$
- 6.8 $L : \mathbf{N} \times \mathbf{N} \rightarrow \mathbf{N} : \langle n, i \rangle \mapsto L'(n, i, \langle 0, n-1 \rangle)$
- 6.9 $L' : \mathbf{N} \times \mathbf{N} \times \mathbf{T}_n \rightarrow \mathbf{N} : \langle n, i, t \rangle \mapsto \begin{cases} 1 + L'(n, i, \text{Left}_n(t)) & \text{when } i \in \text{Left}_n(t) \\ 1 + L'(n, i, \text{Right}_n(t)) & \text{when } i \in \text{Right}_n(t) \\ 0 & \text{when } t = \langle i, i \rangle \end{cases}$
- 6.10 $\text{ordinary}_n : \mathbf{N} \times \mathbf{N} \rightarrow \mathbf{B} : \langle i, j \rangle \mapsto (\langle i, j \rangle \in \mathbf{T}_n) \wedge (j = i + 2^{K(\langle i, j \rangle)} - 1)$
- 6.11 $\left[\begin{array}{l} \text{"ordinary nodes are stable"} \Leftrightarrow \\ \forall t \in \mathbf{N} \times \mathbf{N}; m, n \in \mathbf{N} : (\text{ordinary}_n(t) \wedge m > n) \rightarrow (\text{ordinary}_m(t)) \end{array} \right]$

Figure 6

7/22

- 7.1 $\mathbf{VT}_n = \{N : \mathbf{T}_n \rightarrow \mathbf{H}\}$: set of valued trees
- 7.2 $\left[\begin{array}{l} "N \in \mathbf{VT}_n \text{ is a well-constructed hash tree}" \Leftrightarrow \\ \forall t, u, v \in \mathbf{T}_n : u = \text{Left}_n(t) \wedge v = \text{Right}_n(t) \rightarrow N(t) = \text{NodeHash}_n(t, N(u), N(v)) \end{array} \right.$
- 7.3 $\text{NodeHash}_n : \mathbf{T}_n \times \mathbf{H} \times \mathbf{H} \rightarrow \mathbf{H} : \langle \langle i, j \rangle, x, y \rangle \mapsto F \circ \text{NodeFormat}_n(\langle \langle i, j \rangle, x, y \rangle)$
- 7.4 $\text{NodeFormat}_n : \mathbf{T}_n \times \mathbf{H} \times \mathbf{H} \rightarrow \Sigma^*$: a position - dependent formatting function
- 7.5 $N_{\bar{M}} \in \mathbf{VT}_{\# \bar{M}}$: hash tree generated from leaves \bar{M}
- 7.6 $N_{\bar{M}} : t \mapsto \begin{cases} \text{NodeHash}_{\# \bar{M}}(t, N_{\bar{M}} \circ \text{Left}_{\# \bar{M}}(t), N_{\bar{M}} \circ \text{Right}_{\# \bar{M}}(t)) & \text{when } t \in \mathbf{T}_{\# \bar{M}}^+ \\ M_i & \text{when } t = \langle i, i \rangle \end{cases}$
- 7.7 $\left[\begin{array}{l} "ordinary nodes have stable values" \Leftrightarrow \\ \forall t \in \mathbf{T}_n, \bar{M}, \bar{P} \in \mathbf{H}^+ : (\text{ordinary}_{\# \bar{M}}(t) \wedge \bar{M} \subset \bar{P}) \rightarrow (N_{\bar{M}}(t) = N_{\bar{P}}(t)) \end{array} \right.$
- 7.8 $\left[\begin{array}{l} "hash tree $N \in \mathbf{VT}_n$ is valid for message sequence \bar{M}" \Leftrightarrow \\ N = N_{\bar{M}} \end{array} \right.$

Figure 7

8/22

$$8.1 \quad \text{NodeFormat}_n : \langle \langle i, j \rangle, x, y \rangle \mapsto \begin{cases} \text{RootFormat}(n, x, y) & \text{when } \langle i, j \rangle = \langle 0, n-1 \rangle \\ \text{ParentFormat}(x, y) & \text{when } \langle i, j \rangle \in \mathbf{T}_n^+ \cap \mathbf{T}_n^- \end{cases}$$

$\text{RootFormat}(n, x, y) = "< \text{root}"$

$+ " \text{size} = " + \text{Base10}(n)$

$$8.2 \quad + " \text{left} = " + \text{quote} + \text{Base64}(x) + \text{quote}$$

$+ " \text{right} = " + \text{quote} + \text{Base64}(y) + \text{quote}$

$+ " / > "$

$\text{ParentFormat}(x, y) = "< \text{node}"$

$$8.3 \quad + " \text{left} = " + \text{quote} + \text{Base64}(x) + \text{quote}$$

$+ " \text{right} = " + \text{quote} + \text{Base64}(y) + \text{quote}$

$+ " / > "$

Figure 8

$$9.1 \quad \mathbf{U}_n = \mathbf{T}_n \cup \{P, S\} : \text{node set for combined signature tree}$$

$$9.2 \quad R = \langle 0, n-1 \rangle \in \mathbf{T}_n \subset \mathbf{U}_n : \text{root node of hash tree}$$

$$9.3 \quad \begin{cases} \text{parent}(R) = P \\ \text{parent}(P) = S \end{cases}$$

Figure 9

9/22

- 10.1 $\mathbf{VU}_n = \{N : \mathbf{U}_n \rightarrow \Sigma^*\}$: set of valued trees
- 10.2 $\left[\begin{array}{l} \text{"}N \in \mathbf{VU}_n \text{ is a well-constructed combined signature tree"} \Leftrightarrow \\ N|_{\mathbf{T}_n} \text{ is a well-constructed hash tree"} \\ \wedge N(R) = \text{PadStrip}(N(P)) \\ \wedge \exists d \in \mathbf{K}_D : V_{EG}(d, N(S), N(P)) \end{array} \right.$
- 10.3 $N_{e, \bar{M}, z} \in \mathbf{VU}_{\# \bar{M}}$: combined signature tree generated by $e \in \mathbf{K}_E, \bar{M} \in \mathbf{H}^+, z \in \Sigma^{P-L}$
- 10.4 $N_{e, \bar{M}, z} : u \mapsto \begin{cases} S_{EG}(e, N_{e, \bar{M}, z}(P)) & \text{if } u = S \\ \text{PadFormat}(N_{e, \bar{M}, z}(R), z) & \text{if } u = P \\ N_{\bar{M}}(u) & \text{if } u \in \mathbf{T}_{\# \bar{M}} \end{cases}$
- 10.5 $\left[\begin{array}{l} \text{"combined signature tree } N \in \mathbf{VU}_n \text{ is valid for } d \in \mathbf{K}_D, \bar{M} \in \mathbf{H}^+ \text{"} \Leftrightarrow \\ \text{"}N \text{ is a well-constructed combined signature tree"} \\ \wedge V_{EG}(d, N(S), N(P)) \\ \wedge N(R) = N_{\bar{M}}\langle 0, \# \bar{M} - 1 \rangle \end{array} \right.$

Figure 10

- 11.1 $\text{PadFormat} : \mathbf{H} \times \Sigma^{P-L} \rightarrow \mathbf{J}$: hash value padding function
- 11.2 $\text{PadFormat} : \langle h, z \rangle \mapsto h + z$
- 11.3 $\text{PadStrip} : \mathbf{J} \rightarrow \mathbf{H}$: pad stripping
- 11.4 $\text{PadStrip} : j \mapsto j[0, L-1]$
- 11.5 $\text{Padding} : \mathbf{J} \rightarrow \Sigma^{P-L}$: pad extraction
- 11.6 $\text{Padding} : j \mapsto j[L, P-1]$
- 11.7 "inverse on first parameter" $\Leftrightarrow \forall h, z \in \Sigma^* : h = \text{PadStrip}(\text{PadFormat}(h, z))$
- 11.8 "inverse on second parameter" $\Leftrightarrow \forall h, z \in \Sigma^* : z = \text{Padding}(\text{PadFormat}(h, z))$

Figure 11

10/22

- 12.1 $L = L(n, i); k, i \in [0, n-1]$: sequence parameters
- 12.2 $B_{n,i,0}, B_{n,i,1}, \dots, B_{n,i,L+1} \in T_n$: branch nodes
- 12.3 $S_{n,i,0}, S_{n,i,1}, \dots, S_{n,i,L} \in T_n$: sibling nodes
- 12.4 $side_{n,i,0}, side_{n,i,1}, \dots, side_{n,i,L} \in \{\text{"left"}, \text{"right"}\}$: sibling positions

- 12.5 $B_{n,i,L+1} = \langle 0, n-1 \rangle$: root node
- 12.6 $side_{n,i,k} = \begin{cases} \text{"left"} & \text{when } i \in \text{Right}_n(B_{n,i,k+1}) \\ \text{"right"} & \text{when } i \in \text{Left}_n(B_{n,i,k+1}) \end{cases}$
- 12.7 $S_{n,i,k} = \begin{cases} \text{Left}_n(B_{n,i,k+1}) & \text{when } side_{n,i,k} = \text{"left"} \\ \text{Right}_n(B_{n,i,k+1}) & \text{when } side_{n,i,k} = \text{"right"} \end{cases}$
- 12.8 $B_{n,i,k} = \begin{cases} \text{Right}_n(B_{n,i,k+1}) & \text{when } side_{n,i,k} = \text{"left"} \\ \text{Left}_n(B_{n,i,k+1}) & \text{when } side_{n,i,k} = \text{"right"} \end{cases}$

Figure 12

11/22

- 13.1 $\text{ExtractedSignature} : \mathbf{K}_E \times \mathbf{H}^+ \times \Sigma^{P-L} \times \mathbf{N} \rightarrow \Sigma^*$
- 13.2 $\text{SiblingSeq} : \mathbf{H}^+ \times \mathbf{N} \times \mathbf{N} \rightarrow \Sigma^*$
- 13.3 $\text{ExtractedSignature} : \langle e, \bar{M}, z, t \rangle \mapsto \begin{bmatrix} \text{SignTagStart}(N_{e, \bar{M}, z}(S), z, \# \bar{M}) \\ + \text{SiblingSeq}(\bar{M}, t, 0) \\ + \text{SignTagEnd}() \end{bmatrix}$
- 13.4 $\text{SiblingSeq} : \langle \bar{M}, t, k \rangle \mapsto \begin{cases} \text{SibTag}(\text{side}_{\# \bar{M}, t, k}, N_{\bar{M}}(S_{\# \bar{M}, t, k})) \\ + \text{SiblingSeq}(\bar{M}, t, k+1) \end{cases} \begin{matrix} \text{when } k < L(0, \# \bar{M} - 1) \\ \text{when } k = L(0, \# \bar{M} - 1) \end{matrix}$
- 13.5 $\text{SignTagStart} : \mathbf{J} \times \Sigma^* \times \mathbf{N} \rightarrow \Sigma^* : \langle j, z, n \rangle \mapsto \begin{bmatrix} "< \text{signature}" \\ + " \text{value} =" + \text{quote} + \text{Base64}(j) + \text{quote} \\ + " \text{pad} =" + \text{quote} + \text{Base64}(z) + \text{quote} \\ + " \text{size} =" + \text{Base10}(n) \\ + ">" \end{bmatrix}$
- 13.6 $\text{SignTagEnd} : \rightarrow \Sigma^* : \mapsto "</signature>"$
- 13.7 $\text{SibTag} : \Sigma^* \times \mathbf{H} \rightarrow \Sigma^* : \langle s, v \rangle \mapsto \begin{bmatrix} "<" + s \\ + " \text{value} =" + \text{Base64}(v) \\ + "/" + ">" \end{bmatrix}$

Figure 13

12/22

- 14.1 extracted signature \Rightarrow $\left\{ \begin{array}{l} sig \in \mathbf{J} : \text{signature value} \\ z \in \Sigma^{P-L} : \text{padding bits} \\ n \in \mathbf{N} : \text{stated size of the tree} \\ L \in \mathbf{N} : \text{number of siblings on branch} \\ p_0 \dots p_{L-1} \in \{left, right\} : \text{position indicators} \\ s_0 \dots s_{L-1} \in \mathbf{H} : \text{sibling values} \end{array} \right.$
- 14.2 $XS \in \mathbf{K}_D \times \mathbf{H} \times \mathbf{J} \times \Sigma^{P-L} \times \mathbf{N} \times \mathbf{N} \times \{left, right\}^+ \times \mathbf{H}^+ : \text{extracted signature verification}$
- 14.3 $XS = \langle d, M, sig, z, n, L, \{p_0 \dots p_{L-1}\}, \{s_0 \dots s_{L-1}\} \rangle$
- 14.4 $\mathbf{W}_L = \{S_0 \dots S_{L-1}, B_0 \dots B_L, P\} : \text{nodes of the base tree of a verification tree}$
 $\text{parent}(S_i) = B_{i+1}$
- 14.5 $\text{parent}(B_i) = B_{i+1}, \text{ when } i < L$
 $\text{parent}(B_L) = P$: edges of the base tree of a verification tree
- 14.6 $N_{XS} \in \mathbf{VW}_L = \{N : \mathbf{W}_L \rightarrow \Sigma^*\} : \text{verification tree}$
- 14.7 $N_{XS} : w \mapsto \begin{cases} M & \text{when } w = B_0 \\ S_i & \text{when } w = S_i \\ \text{NodeHash}_n(P(B_i), N_{XS}(S_{i-1}), N_{XS}(B_{i-1})) & \text{when } w = B_i, 0 < i \leq L, p_i = left \\ \text{NodeHash}_n(P(B_i), N_{XS}(B_{i-1}), N_{XS}(S_{i-1})) & \text{when } w = B_i, 0 < i \leq L, p_i = right \\ \text{PadFormat}(N_{XS}(B_L), z) & \text{when } w = P \end{cases}$
- 14.8 $P_{XS} : \{B_0 \dots B_L\} \rightarrow T_n : w \mapsto \begin{cases} \text{Left}_n(B_{i+1}) & \text{when } w = B_i, i < L, p_i = right \\ \text{Right}_n(B_{i+1}) & \text{when } w = B_i, i < L, p_i = left \\ \langle 0, n-1 \rangle & \text{when } w = B_L \end{cases}$
- 14.9 "signature is valid for $\langle d, M \rangle$ " $\leftrightarrow \begin{cases} \text{"signature is well-formed"} \\ \wedge P_{XS}(B_0) \text{ is defined} \\ \wedge \exists i : P_{XS}(B_0) = \langle i, i \rangle \\ \wedge V_{EG}(d, sig, N_{XS}(P)) \end{cases}$

Figure 14

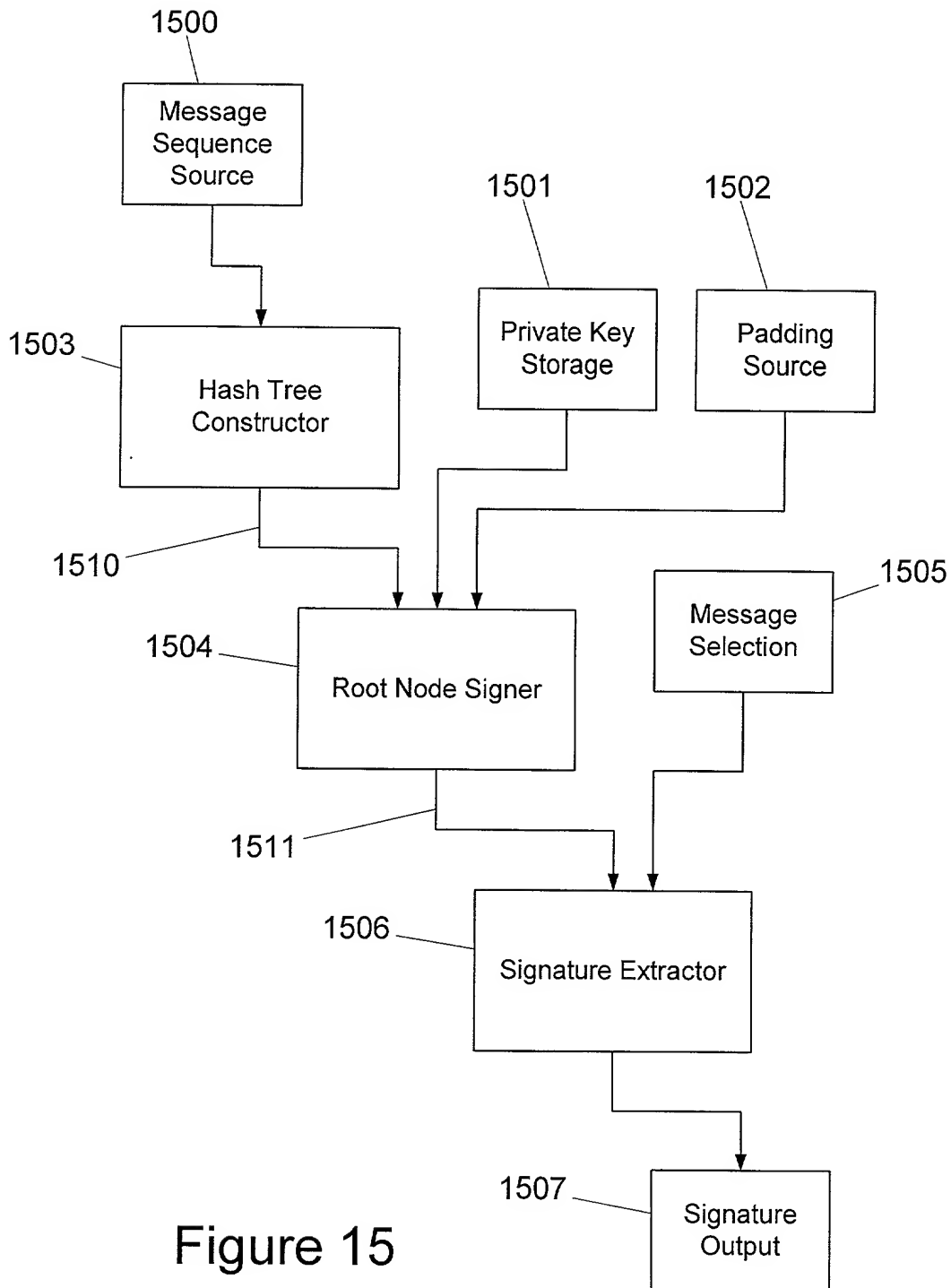


Figure 15

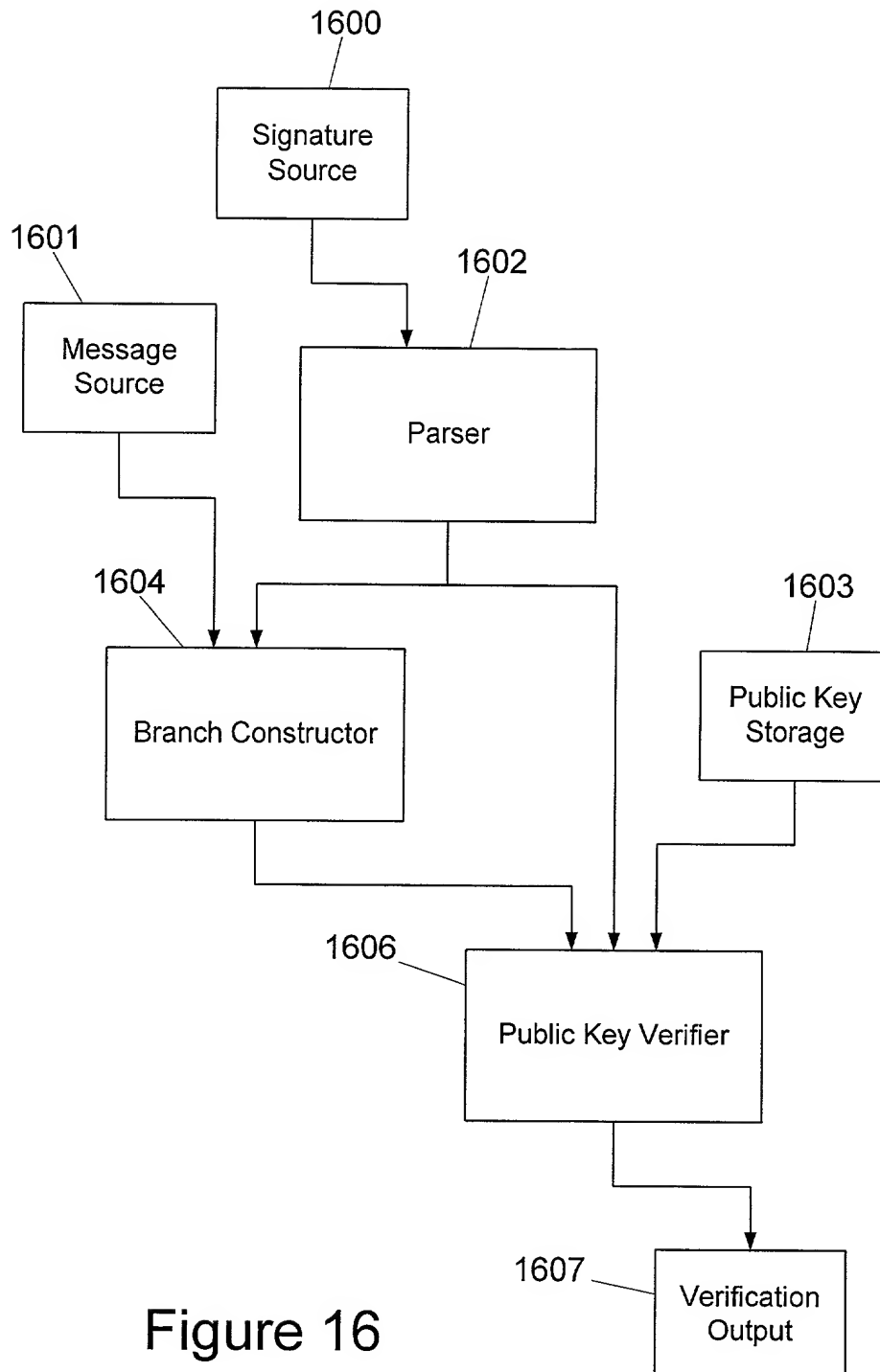


Figure 16

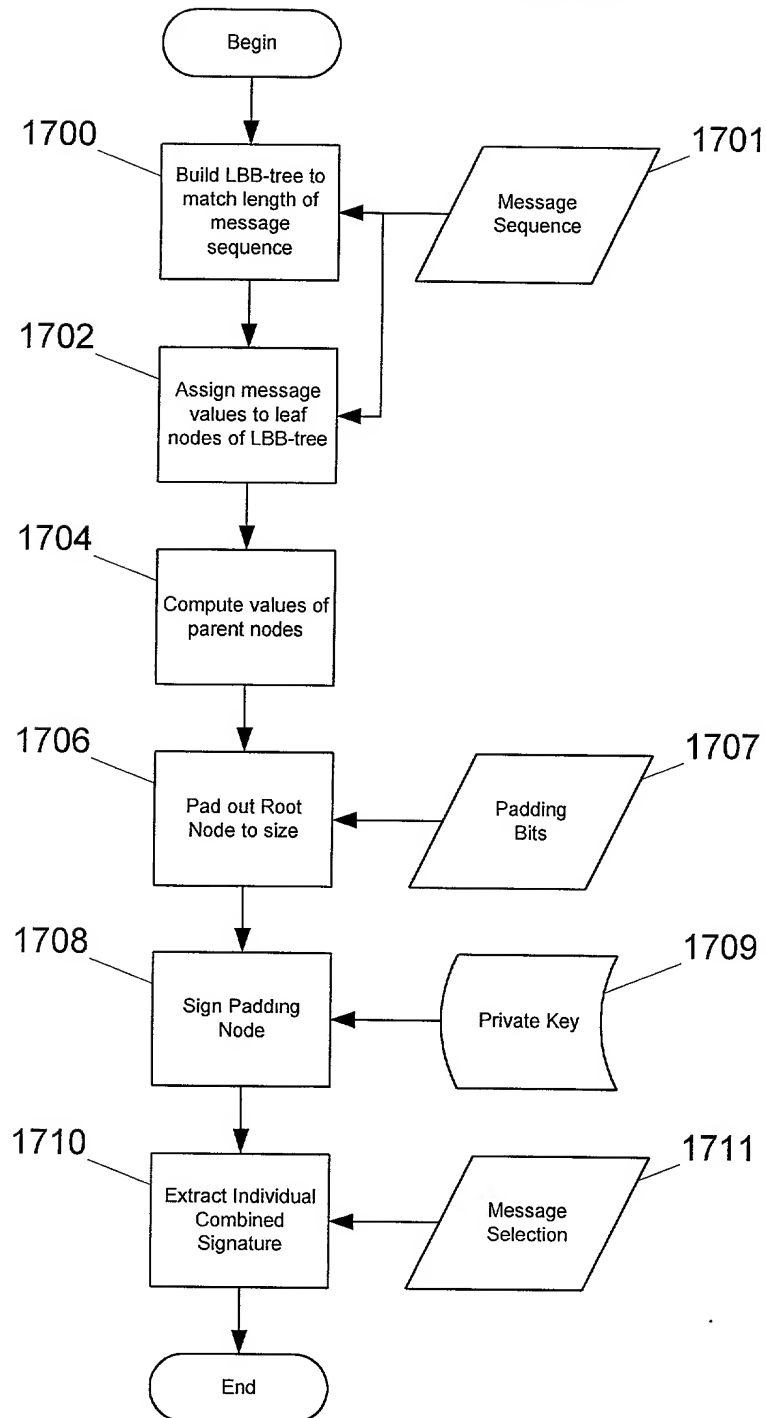


Figure 17

16/22

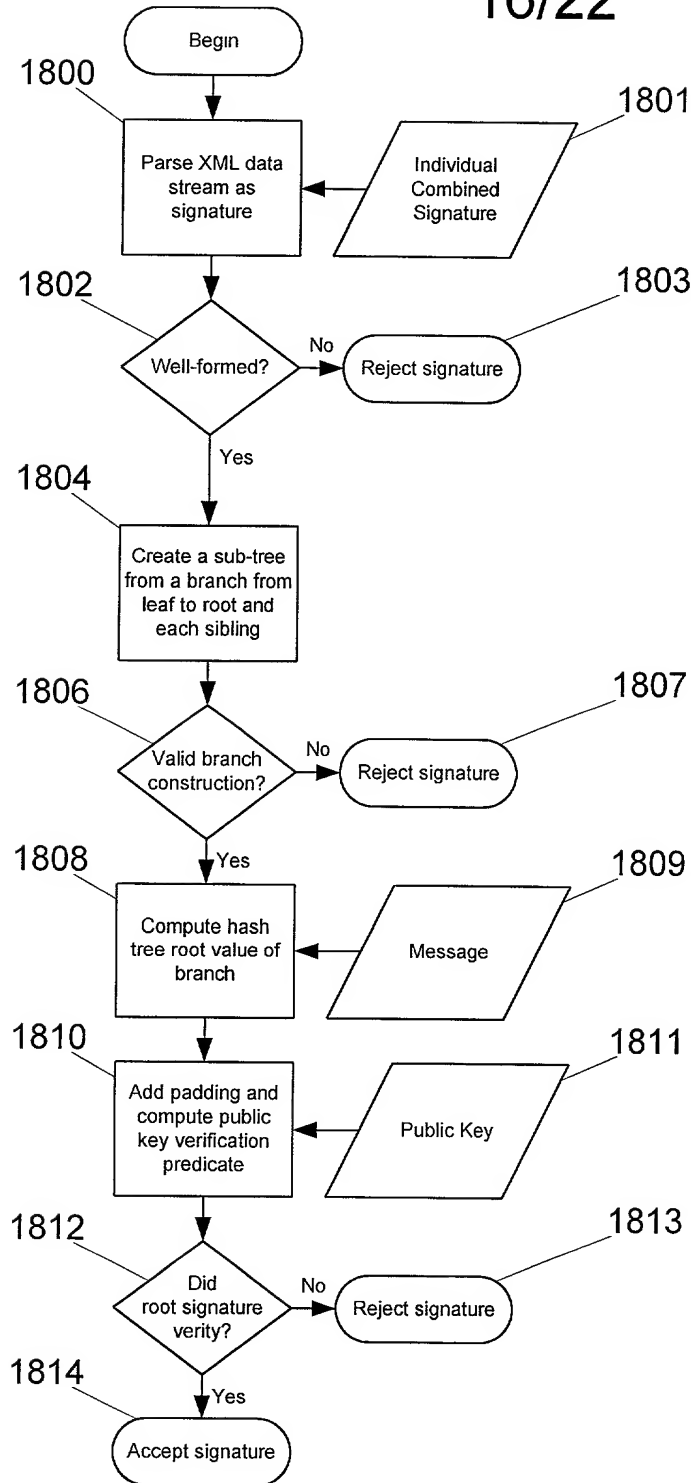


Figure 18

17/22

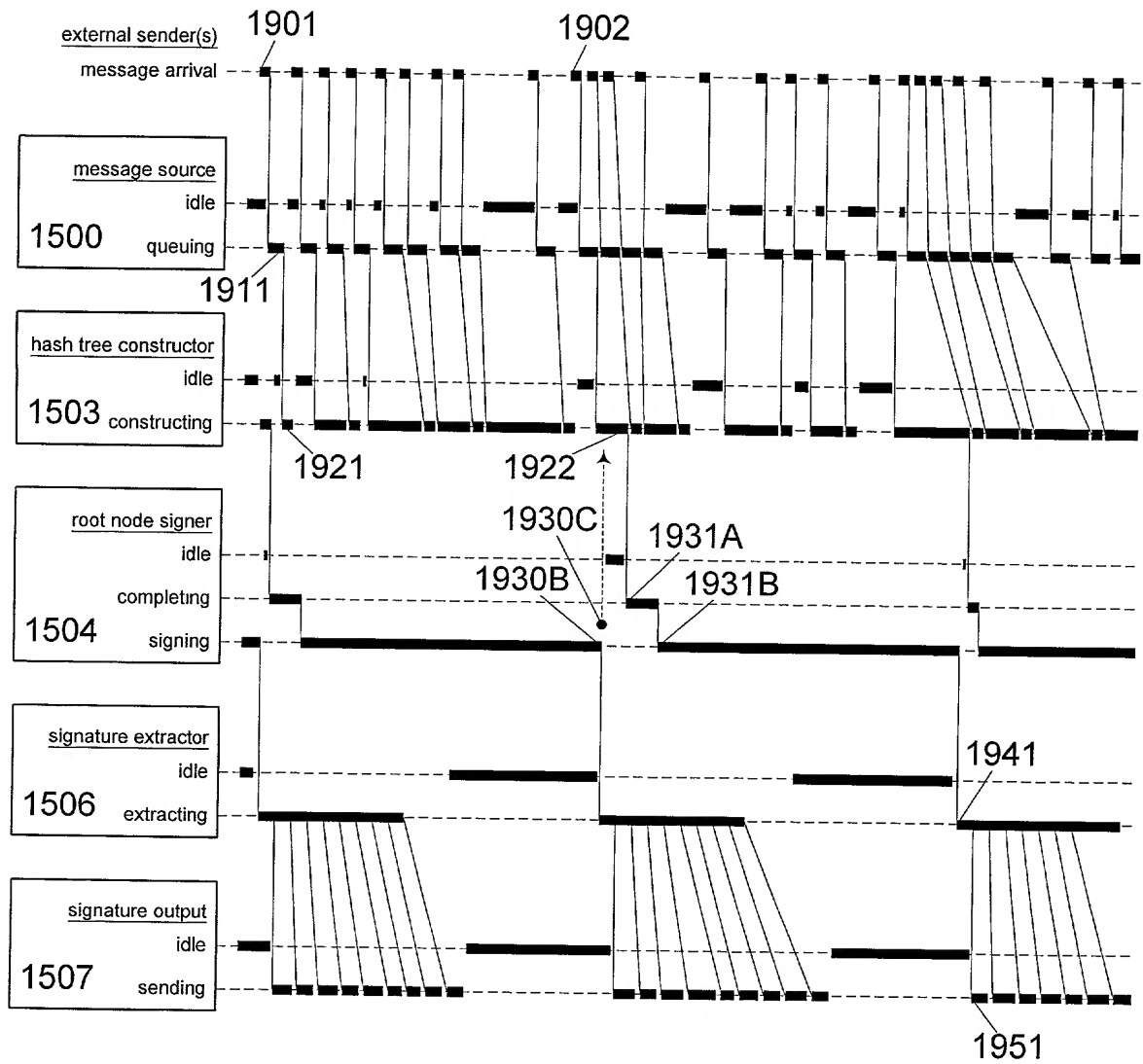


Figure 19

18/22

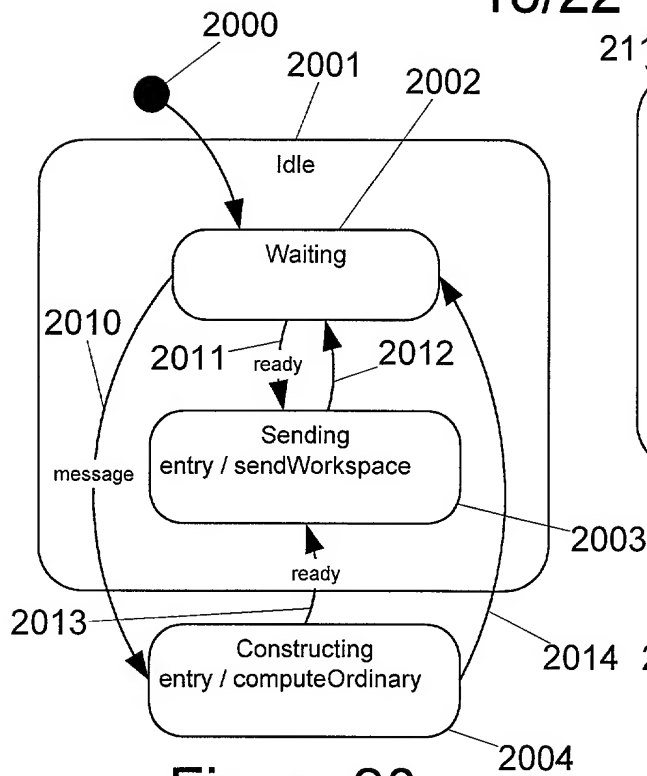


Figure 20

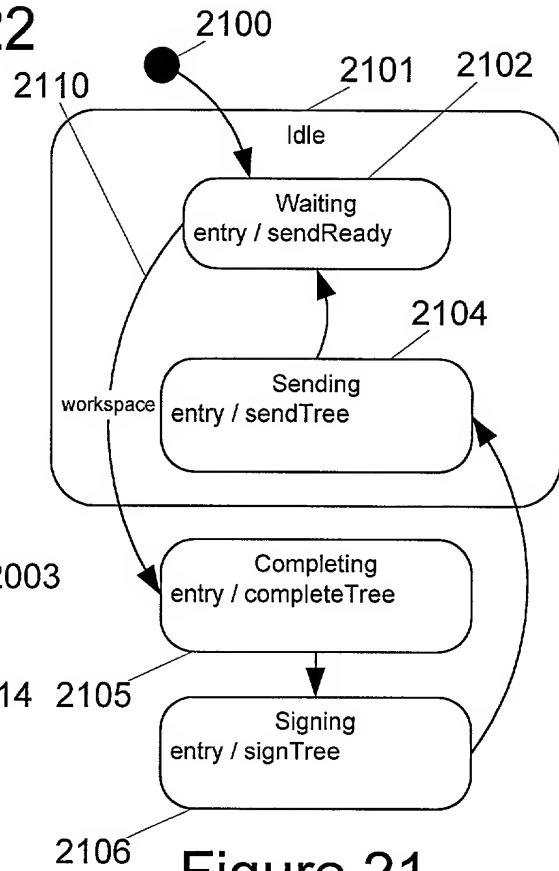


Figure 21

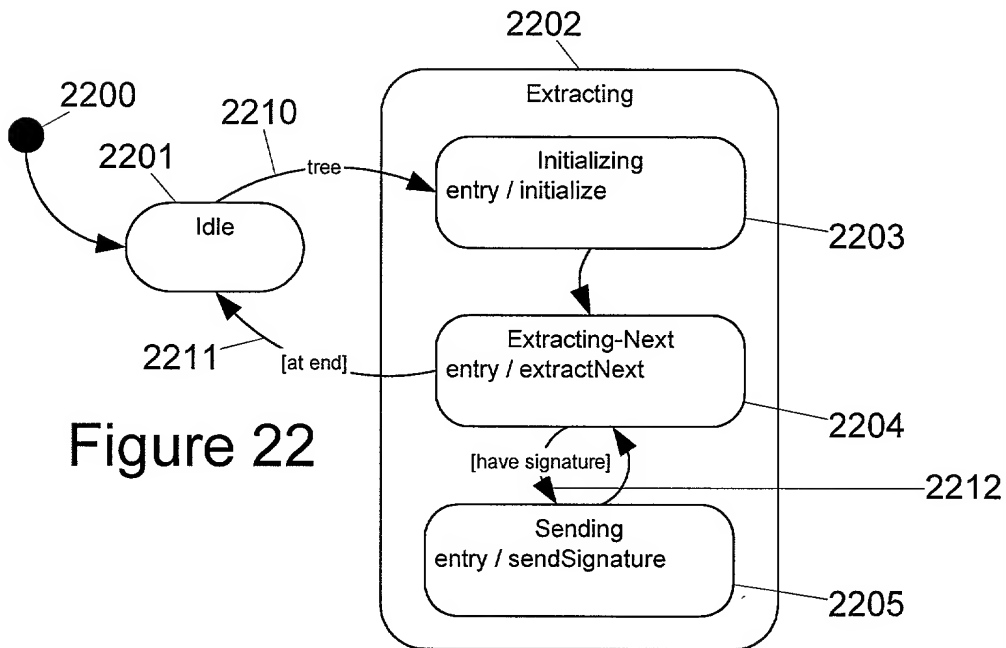


Figure 22

19/22

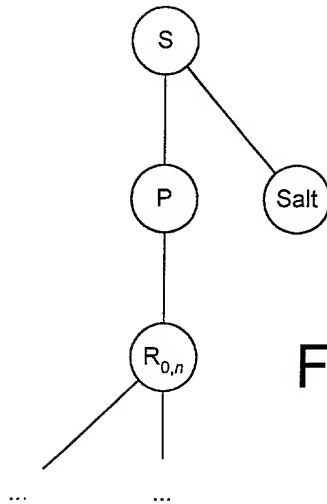


Figure 23A

23.7.3 $\text{NodeHash}_{n,\text{salt}} : \mathbf{H} \times \mathbf{H} \rightarrow \mathbf{H} : \langle x, y \rangle \mapsto F(\text{salt} + \text{NodeFormat}_n(x, y))$

23.13.5 $\text{SignTagStart} : \mathbf{J} \times \mathbf{H} \rightarrow \Sigma^* : \langle j, \text{salt} \rangle \mapsto \left[\begin{array}{l} "< \text{signature}" \\ + \text{"value ="} + \text{quote} + \text{Base64}(j) + \text{quote} \\ + \text{"salt ="} + \text{quote} + \text{Base64}(\text{salt}) + \text{quote} \\ + ">" \end{array} \right]$

Figure 23B

24.8.1 $\text{NodeFormat}_n : (\langle i, j \rangle, x, y) \mapsto \begin{cases} \text{LayerFormat}(\text{"bottom"}, x, y) & \text{when } |i - j| = 1 \\ \text{LayerFormat}(\text{"top"}, x, y) & \text{otherwise} \end{cases}$

$\text{LayerFormat}(\text{name}, x, y) = "<" + \text{name} +$

24.1 $\begin{aligned} &+ \text{"left ="} + \text{quote} + \text{Base64}(x) + \text{quote} \\ &+ \text{"right ="} + \text{quote} + \text{Base64}(y) + \text{quote} \\ &+ \text{" />"} \end{aligned}$

Figure 24

20/22

25.8.1 $\text{NodeFormat}_n : (\langle i, j \rangle, x, y) \mapsto$

$\begin{aligned} & "< \text{node}" + \\ & + " \text{pos} =" + \text{Base10}(i) + ", " + \text{Base10}(j) \\ & + " \text{left} =" + \text{quote} + \text{Base64}(x) + \text{quote} \\ & + " \text{right} =" + \text{quote} + \text{Base64}(y) + \text{quote} \\ & + "/" >" \end{aligned}$
--

Figure 25

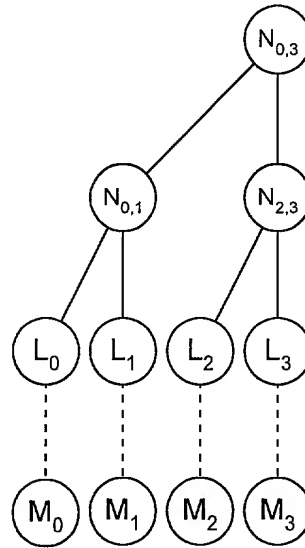


Figure 26A

26.7.6 $N_{\overline{M}} : t \mapsto \begin{cases} \text{NodeHash}_{\# \overline{M}}(t, N_{\overline{M}} \circ \text{Left}_n(t), N_{\overline{M}} \circ \text{Right}_n(t)) & \text{when } t \in \mathbf{T}_{\# \overline{M}}^+ \\ \text{LeafHash}(M_i) & \text{when } t = \langle i, i \rangle \end{cases}$

26.1 $\text{LeafHash} : \mathbf{N} \times \mathbf{H} \rightarrow \mathbf{H} : x \mapsto F(\text{LeafFormat}(x))$

$\text{LeafFormat}(x) = "< \text{leaf}"$

26.2 $\begin{aligned} & + " \text{value} =" + \text{quote} + \text{Base64}(x) + \text{quote} \\ & + "/" >" \end{aligned}$

Figure 26B

21/22

```
2771T [ <signature
      2771 [ value=". . ."
      2773 [ size=13
            >
```

Figure 27

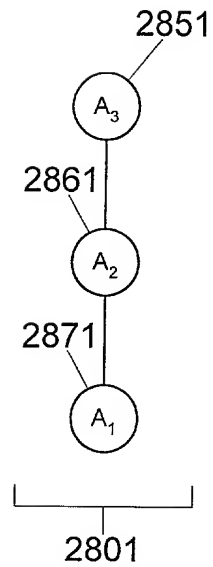
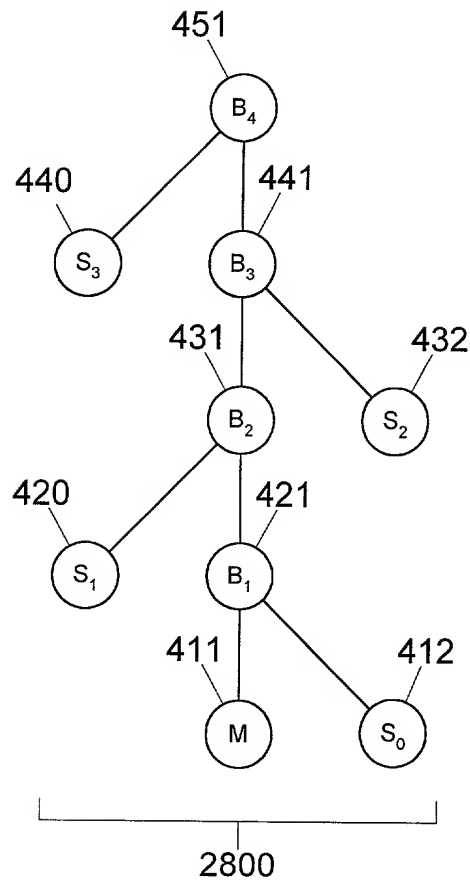


Figure 28

- 29.1 $\mathbf{W}'_L = \mathbf{W}_L \setminus P$: nodes of the base tree of a verification tree
- 29.2 $N'_{XS} = N_{XS}|_{\mathbf{W}'_L}$: verification tree
- 29.3 $V_{MR} : \mathbf{K}_D \times \mathbf{J} \rightarrow \mathbf{J}$: message recovery operation for signature verification
- 29.14.9 "signature is valid for $\langle d, M \rangle$ " \leftrightarrow

$$\begin{cases} \text{"signature is well - formed"} \\ \wedge P_{XS}(B_0) \text{ is defined} \\ \wedge \exists i : P_{XS}(B_0) = \langle i, i \rangle \\ \wedge \text{PadStrip} \circ V_{MR}(d, sig) = N_{XS}(B_L) \end{cases}$$

Figure 29